DOE HEADQUARTERS COMPUTER SYSTEM SECURITY CERTIFICATION and APPROVAL CHECKLIST

COMPUTER SYSTEM SECURITY CERTIFICATION/APPROVAL CHECKLIST

System Type:			Host:		
System Name:			Owner:		
<u>AC</u>	<u>PPM</u>				
(1)		Security objectives were	established by the owner during the planning phase of the life cycle.		
(2)		Security requirements were defined by the developer to support the security objectives.			
(3)		Design features enforce the security requirements.			
(4)		Testing has been conduc	Testing has been conducted to test all the security design features and the results are recorded.		
(5)		Security tests were conducted satisfactorily or a statement of acceptance of risk has been issued by the owner. (There may be residual risks even though tests were found to be satisfactory.)			
(6)		Appropriate data set protect by higher authority.	Appropriate data set protection rules, authorities, and USERIDs have been established by the owner or as mandated by higher authority.		
(7)		Access control protection	Access control protection has been incorporated and has been turned over to system operations.		
(8)		All manufacturer generic	All manufacturer generic, test team, temporary, and superfluous passwords have been deleted.		
(9)		All privacy, freedom of in	All privacy, freedom of information, sensitivity, and classification considerations have been identified and resolved		
(10)		Host system testing (mainframe, mini-computer, LAN server), has verified that all security controls are effective a that host system security controls support the system/application.			
(11)		A Computer Security & Privacy Plan (CSPP) has been developed for the host system and has been updated to reflect this system/application or information has been supplied to the appropriate ACPPM of the host system.			
(12)	_	Documentation identifying	ng risk has been reviewed for the host system facility.		
			ACPPM SECURITY CERTIFICATION		
satisfac	tory level o	f operational security is presen	wed to substantiate security controls applied to the system/application. As of this date, a t and the application/system can operate under reasonable risk. Any subsequent changes, edures will require re-evaluation to determine if changes have occurred affecting security.		
can/ca	annot opera	ate under reasonable risk. Thi	satisfactory level of operational security is / is not present and that the application/system s certification is valid for three years / invalid . Any subsequent changes, modifications as will make this certification null and void.		
Certifie	er:		Date:		
		ACPPM	Organization		
			APPROVAL TO PROCESS		
			M certification approval/disapproval, I accept the inherent risk identified and approve this period of three years, or until a modification affecting the protective controls occurs.		
Approv	ver:	Program Manager	Date:		
		Program Manager	Organization		

DOE HEADQUARTERS COMPUTER SYSTEM SECURITY CERTIFICATION and APPROVAL CHECKLIST

INSTRUCTIONS FOR USE

- 1. This checklist provides guidance to the Assistant Computer Protection Program Manager (ACPPM) for performing security certification on either new or significantly modified general support systems and/or major applications. It follows the security portions of the DOE Guide 200.1-01, *Software Engineering Methodology (SEM)*.
- 2. The ACPPM has the responsibility for security design and preparation for system documentation for certification and approval.
- 3. The ACPPM will complete this checklist in conjunction with other involved personnel (e.g., application user, developer, computer operations, CPPM) during the development process.
- 4. The checklist must be completed and certified by the ACPPM, and approved by the Program Manager prior to processing live data in an operational environment.
- 5. The completed checklist will become a part of the system master documentation and considered to be the security certification document and official management approval to operate. It will remain the final certification document until the system is modified to the extent that the security controls are altered. In that event, another checklist will be completed, approved, and attached to the master documentation and the Computer Security and Privacy Plan (CSPP).